# Background

# Pre-requisites

Valid domain user.

# Risks

# How to check for

Check for users that have unconstrained delegation. Default such users are the domain controllers machine account, in other words, the domain controller computer objects. The account needs to have `UserAccountControl` attribute set to `TRUSTED_FOR_DELEGATION`. If you use ADExplorer it might be a bit difficult to know if the user has this attribute set, because the attribute value is set as an integer.

If you are able to compromise users that have unconstrained delegation

```
MATCH (c:Computer {unconstraineddelegation:true}) return c
```

With powerview you can check for computers accounts with unconstrained delegation like this:

```
get-domaincomputer -unconstrained | select-object -property name,useraccountcontrol
```

With PowerView you can check for users with unconstrained delegation like this:

```
Get-DomainUser -ldapfilter "(userAccountControl:1.2.840.113556.1.4.803:=524288)"
```

# How to exploit

# Recommendation

# Related Vulnerabilities

# References

https://dirkjanm.io/krbrelayx-unconstrained-delegation-abuse-toolkit/